NY Zelle Suit Highlights Fraud Risks Of Electronic Payments

By **Timothy Ofak, Joseph Katz, and Augustus Calabresi** (October 15, 2025)

Timothy Ofak

Joseph Katz

Augustus Calabresi

As financial transactions occur with increased regularity through nontraditional channels such as electronic payment applications, financial service providers must remain cognizant of the potential risks that arise. An August enforcement action filed by the New York attorney general highlights these risks.

The Rise of Electronic Payment Networks

In a complaint filed in August in New York state court, New York Attorney General Letitia James contends that Early Warning Services LLC, or EWS — a company that several major banks collectively organized — has created an atmosphere that is conducive to fraud with its electronic payment application, Zelle.

The complaint characterizes the relevant history as follows. Until recently, consumers seeking to send money (other than in cash) generally needed to go through a bank to process a check, wire transfer or automated clearing house payment.

This paradigm began to shift with the advent of electronic payment applications (such as PayPal, Venmo and Cash App). In response, several large banks, including JPMorgan Chase, Bank of America and Wells Fargo, organized EWS to offer more accessible banking services.

In turn, EWS developed Zelle, which is a service that provides access to an instant payment network through a website or mobile application.

To create an account, Zelle requires only an email address or telephone number, either of which is referred to as a token, and a bank account. There is no enrollment fee. A user can sign up for multiple accounts and associate as many as five tokens with one bank account.

Previously, a user could associate more than five tokens with one bank account. No other verification is required. Several major banks also automatically integrate Zelle with their websites and mobile applications, which means that users do not need to download any additional application.

A user transfers funds through Zelle by entering the recipient's token and the amount of money to be transferred. If the token is registered — that is, a user entered that email or phone number when enrolling in the service — EWS deposits the money into the bank account associated with the recipient's token in near real time. EWS then notifies the relevant banks of the transfer.

If the token is unregistered, EWS sends a message to the email or phone number entered, advising the owner that they can access the transferred funds by enrolling in Zelle. At the end of each day, the participating banks resolve settlement of the day's transfers among

themselves.

Allegations of an Atmosphere Conducive to Fraud

In support of her contention that EWS created an atmosphere that is conducive to fraud, the New York attorney general recites the following allegations: Registering for Zelle is frictionless because the service requires only an email or phone number and bank account, charges no registration fee, and is integrated with several large banks' existing websites and mobile applications.

The simplicity of the registration process, the attorney general maintains, makes it easier for users to engage in fraudulent conduct.

For example, Zelle requires a participating bank to display only a user's first name, so a party to a transaction has limited identifying information about the other party. This anonymity makes it difficult to verify the recipient in a transfer and track down a user who is inducing fraudulent transfers.

Additionally, because Zelle transfers funds immediately, it is difficult for a user who later realizes that they had erroneously sent funds to undo the transfer. Moreover, because Zelle allows one user to link up to five tokens to one bank account and change with which bank account a token is associated, each token of a user engaging in fraudulent conduct may not appear as suspicious.

And even when a user reports fraud with respect to one token, Zelle allegedly still allows accounts with which the reported token is associated to use other tokens. Further, an unauthorized person need only gain access to a one-time passcode generated to recover an account for that person to access a user's Zelle account and connect it to a different bank account.

EWS established this network, the attorney general maintains, knowing that its design and features unduly expose users to fraudulent activity. For example, EWS and participating banks have allegedly had the technical capability to block a user from transferring funds to certain tokens. Participating banks also have allegedly been able to halt certain transactions that they determine to be suspicious or risky.

And according to the attorney general, not until several years after the applicatoin's debut did EWS prohibit users from registering with email addresses that appeared to be associated with banks, government entities or Zelle.

Although EWS promulgated rules governing use of the Zelle network, the attorney general asserts that these rules were inadequate and were not meaningfully enforced. Likewise, the attorney general seeks to hold EWS liable for removing even the "modest" network security protections that it had implemented in 2019.

EWS has yet to file a dispositive motion or responsive pleading, and the case remains pending before the Supreme Court of the State of New York, County of New York, the state trial court in Manhattan.

Implications for Financial Service Providers

This action demonstrates the need for financial service providers to carefully balance accessibility with consumer protection. Part of what has made electronic payment

applications, including Zelle, so popular is their ease of use.

It is easier to open a mobile application than it is to write and mail a paper check or initiate a wire transfer. Yet it is this same ease of use that, according to the attorney general, has facilitated fraud across the Zelle network.

Thus, companies should take care to include robust cybersecurity protections and network safeguards when designing widely accessible electronic applications that provide consumer financial services.

These safeguards should include security features for managing individual accounts as well as moderating interactions between users.

Notably, the complaint seeks to impose liability on Zelle for its account design, which allegedly allows an unauthorized person to easily obtain access to a user's account.

To mitigate this risk, companies should consider procedures like mandatory two-factor authentication to log in to an account, update account information (like the bank account associated with the service) and process a transaction. Such an additional step makes it more difficult for an unauthorized person to access a user's account and divert money from that account.

Separately, the complaint seeks to impose liability on Zelle for not taking sufficient measures to protect users from unwittingly engaging in fraudulent transactions. As examples, the complaint cites the lack of information about other users that Zelle displays and that Zelle previously allowed users to register email addresses that falsely appeared to be associated with a bank, government or Zelle.

To mitigate this risk, companies should consider procedures like requiring users to provide and verify certain identifying information and to disclose such information to other users. Providing such information allows one to more easily confirm the identity and legitimacy of another party to a transaction.

Additionally, this action highlights the importance of establishing clear policies and procedures concerning the use of financial technology products. As discussed, the attorney general assigned significant weight to the EWS board's allegedly insufficient rules governing the use of Zelle and decision to revoke supposedly critical network safeguards.

Maintaining appropriate policies and procedures and adhering to those policies and procedures remain critical elements of a compliance program. This point is particularly important with respect to newer financial technology products whose risks may not yet be fully known.

Thus, it is also important to perform regular reviews of policies and procedures to ensure that they account for the current consumer environment, in addition to government regulations and guidance.

Further, it may be prudent to educate consumers regarding these risks. For example, wire fraud advisory notices are standard practice in many transactions involving large transfers of money, such as when purchasing a home.

Likewise, it may be prudent to warn consumers about the specific risks of products like electronic payment applications if the company accepts payment using these means.

Of final note, the investigation into Zelle did not originate with the New York attorney general's office. The Consumer Financial Protection Bureau and several U.S. senators began investigating alleged fraud over the Zelle network years earlier.

Only after the CFPB dismissed the case with prejudice as to all defendants, including three participating banks (JPMorgan Chase, Bank of America and Wells Fargo) that the New York attorney general did not name as defendants, in March 2025 did the New York attorney general file the current action.

This case, therefore, highlights the ability and appetite of state regulators to pursue actions in which the CFPB has little interest or has abandoned.

Conclusion

Because the case remains pending, it is too soon to draw any legal conclusion from this case. For example, the court may determine that EWS lacked the requisite knowledge for its actions to legally constitute fraud. And significant portions of the complaint have been redacted, so a court order may turn on facts that are not yet publicly known.

The fraud claim under New York state law is also more specific than the various federal law claims that the CFPB had alleged in its action. So regardless of how this case resolves, we will not know whether the conduct would be viewed differently under federal law.

In any event, this action highlights important compliance policy considerations moving forward.

Timothy P. Ofak is a member, Joseph M. Katz is counsel and Augustus G. Calabresi is an associate at Weiner Brodsky Kider PC.